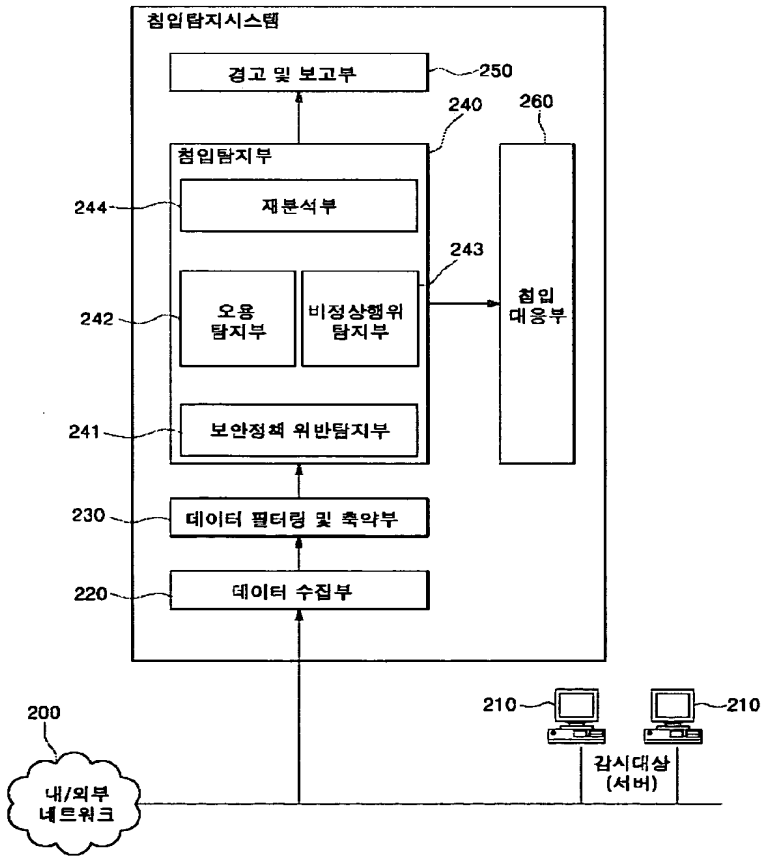
KOREAN PATENT ABSTRACTS(KR)

Document Code:A
(11) Publication No.1020020062070 (43) Publication.Date. 20020725
(21) Application No.1020010003295 (22) Application Date. 20010119
(51) IPC Code:
G06F 15/00

(71) Applicant:
INFOSEC TECHNOLOGIES CO., LTD.
(72) Inventor:
KIM, DONG UK
KIM, GI HYEON
YANG, SEUNG HO
(30) Priority:

(54) Title of Invention
SYSTEM AND METHOD FOR DETECTING INTRUSION USING DIVERSE INTRUSION DETECTION MODEL

Representative drawing



(57) Abstract:

PURPOSE: A system and a method for detecting the intrusion using the diverse intrusion detection models are provided to detect a case violating a security policy set by introducing a traditional access control technology to the intrusion detection system.

CONSTITUTION: The intrusion detection system comprises a data collector, a data filtering and condensing part(230), an intrusion detector(240), a warning and reporting part, and an intrusion responding part (260). The data collector collects all traffics to a network having a monitoring target server(210) from an external or internal network(200) and transfers the collected data to the data filtering and

condensing part. The data filtering and condensing part filters only the traffics to a monitoring target system, and converts and condenses the data to detect the intrusion by extracting the data necessary for the intrusion detection. If the intrusion detector judges the intrusion, the warning and reporting part reports the warning and the related inspection records and the intrusion responding part carries out the defined responding activity such as the environment resetting of the access control system.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.
G06F 15/00

(11) 공개번호 특2002-0062070
(43) 공개일자 2002년07월25일

(21) 출원번호 10-2001-0003295
(22) 출원일자 2001년01월19일

(71) 출원인 주식회사 정보보호기술
대한민국
137-070
서울특별시 서초구 서초동 1337-6 포런빌딩 5층 502

(72) 발명자 김기현
대한민국
463-010
경기도성남시분당구정자동198번지우성아파트615동301호

김동욱
대한민국
157-014
서울특별시강서구화곡4동488-45호

양승호
대한민국
420-101
경기도부천시원미구역곡1동247-2동성아파트311호

(74) 대리인 특허법인아주(대표변리사정은섭)
정은섭

(77) 심사청구 있음

(54) 출원명 다양한 침입탐지모델을 사용하는 침입탐지시스템 및 그 방법

요약

본 발명은 다양한 침입탐지모델을 사용하는 침입탐지시스템 및 그 방법에 관한 것으로, 보다 상세하게는 종래의 오용탐지와 비정상행위탐지로만 구성되는 침입탐지기능에 보안정책위반 탐지 기능과 재분석 기능을 추가하여 침입탐지율을 높이고, 오판율을 줄이며 빠른 침입탐지와 대응기능을 제공할 수 있도록 다양한 침입탐지모델을 사용하는 침입탐지시스템 및 그 방법에 관한 것이다.

대표도

도2

색인어

침입탐지시스템, 보안정책 위반탐지부, 재분석부

명세서

도면의 간단한 설명

도 1은 종래의 침입탐지시스템의 구성을 설명하기 위한 블록구성도이고,

도 2는 본 발명에 따른 침입탐지시스템의 구성을 설명하기 위한 블록구성도이고,

도 3은 본 발명에 따른 침입탐지시스템의 상호동작을 설명하기 위한 상호동작도이고,

도 4는 본 발명에 따른 데이터 필터링 및 축약부와 보안정책위반탐지부를 설명하기 위한 흐름도이고,

도 5는 본 발명에 따른 오용탐지부를 설명하기 위한 흐름도이고,

도 6은 본 발명에 따른 비정상행위탐지부를 설명하기 위한 흐름도이고,

도 7은 본 발명에 따른 결과조정 및 감사데이터 생성부를 설명하기 위한 흐름도이고,

도 8은 본 발명에 따른 재분석부를 설명하기 위한 흐름도이고,

도 9는 본 발명의 다른 실시예에 따른 침입탐지시스템의 상호동작을 설명하기 위한 상호동작도이다.

·* 도면의 주요 부분에 대한 부호 설명 *

200 : 내/외부 네트워크 210 : 감시대상서버

220 : 데이터수집부 230 : 데이터 필터링 및 축약부

240 : 침입탐지부 241 : 보안정책위반탐지부

242 : 오용탐지부 243 : 비정상행위탐지부

244 : 재분석부 250 : 경고 및 보고부

260 : 침입대응부

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 침입탐지시스템에 관한 것으로, 보다 상세하게는 종래의 오용탐지와 비정상행위탐지로만 구성되는 침입탐지기능에 침입차단시스템(Firewall)등에서 사용하는 접근통제 개념을 침입탐지시스템에 도입하여 기관의 시스템/네트워크별 보안정책을 침입탐지시스템에 수용하고, 위반사항을 탐지할 수 있는 기능을 제공하며, 중복 알람 방지와 복합 공격 분석을 위한 재분석 기능을 부가하여 다중 침입시스템을 구성함으로써, 침입탐지 및 대응시간을 단축시키고 시스템의 부하를 줄이면서 정확한 침입분석 능력을 갖도록 하는 다양한 침입탐지모델을 사용하는 침입탐지시스템 및 그 방법에 관한 것이다.

초기에 컴퓨터 시스템 관리자들은 막대한 양의 감사 기록(audit record) 정보들로부터 보안 관리에 필요한 정보들만을 선택적으로 수용하고 분석하기 위해서 일일이 저장된 로그 파일들을 수작업으로 처리해야 했다. 이에 따라, 이를 신속하게 처리하기 위한 자동화된 감사 도구의 개발이 요구되었으며, 그 동안에 축적된 감사 기록 분석 기술을 이용하여 감사기록을 자동으로 분석하여 시스템에 불법적으로 침입하거나 해를 끼친 행위들을 찾아내려는 시도를 하게 되었다. 하지만 사후에 발견되는 침입행위는 늦은 감이 없지 않았고, 해커들의 감사 기록 삭제 시도로 인해 사고 분석 및 발견이 용이하지 않다는 문제점이 존재하였다.

또한, 분산 환경과 개방 환경으로 컴퓨팅 환경이 전환되면서 고도화되고 분산된 공격형태를 취하고 있는 침입 기법으로부터 시스템을 보호하기 위해서는 실시간으로 침입을 탐지하고 대응할 수 있는 실시간 침입탐지시스템을 필요로 하게 되었다.

1980년 초 Anderson은 침입(Intrusion)을 컴퓨터가 사용하는 자원의 무결성(integrity), 비밀성(confidentiality), 가용성(availability)을 저해하는 일련의 행위들의 집합을 의미하며, 컴퓨터 시스템의 보안정책을 파괴하는 행위로 정의하였으며, 1987년 침입탐지시스템의 일반적 모델을 정의한 Dorothy E. Denning은 침입탐지시스템을 대상시스템에서 허가되지 않거나 비정상적인 행위에 대하여 탐지, 식별하고 보고하는 기능의 소프트웨어로 정의하고 있다.

이러한 침입탐지시스템을 크게 다음의 두 가지 분류 기준으로 나누고 있다.

하나는 데이터 소스(Source)를 기반으로 하는 분류 방법이며 다른 하나는 침입탐지 모델을 기반으로 하는 분류 방법이다.

데이터 소스(Source)를 기반으로 침입탐지시스템을 분류하면 호스트 기반(Host Based)과 네트워크 기반(Network Based)을 분류된다. 호스트 기반 침입탐지시스템은 호스트로부터 생성되고 수집된 감사(audit) 데이터를 침입 여부 판정에 사용하며, 하나의 호스트를 탐지영역으로 한다. 네트워크 기반 침입탐지시스템은 네트워크의 패킷 데이터를 수집하여 침입 여부 판정에 사용하며, 침입탐지시스템이 설치된 네트워크 영역 전체를 탐지 대상으로 한다.

침입탐지 모델을 기반으로 분류하면 오용 탐지(Misuse Detection)와 비정상행위 탐지(Anomaly Detection) 기술로 분류된다. 오용탐지는 시스템의 알려진 취약점들을 이용하여 공격하는 행위들을 사전에 공격에 대한 특징 정보를 가지고 있다가 탐지하는 방법으로, 시스템 감사기록 정보에 대한 의존도가 높고 상대적으로 구현 비용이 저렴하나, 알려진 공격기법에 대한 탐지능력만을 가지고 있기 때문에 최신 공격기법에 대한 계속적인 연구가 필요하며, 침입 시나리오를 추가시켜주어야 하는 어려움이 있다. 비정상행위 탐지는 정상적인 시스템 사용에 관한 프로파일과 시스템 상태를 유지하고 있다가, 이 프로파일에서 벗어나는 행위들을 탐지하는 방법으로, 정상적인 프로파일을 생성하는 데 있어 기존의 많은 데이터를 분석하여야 하기 때문에 상대적으로 구현 비용이 크다.

일반적으로 침입탐지시스템(Intrusion Detection System ; IDS)이라 함은 컴퓨터 시스템의 비정상적인 사용, 오용, 남용 등을 가능하면 실시간으로 탐지하는 시스템을 말한다. 이러한 침입탐지시스템에서의 기술적 관건은 컴퓨터 시스템의 침입 여부를 판단하기 위한 근거를 어디에서, 얼마나 정확하게, 그리고 신속하게 찾을 수 있느냐에 달려있다. 그리고 침입 판정시 오판율을 줄이는 문제도 기술적으로 지속적인 성능향상을 통해 해결해야 할 큰 과제이다.

도 1은 종래의 침입탐지시스템의 구성을 설명하기 위한 블록구성도이다.

여기에 도시된 바와 같이, 데이터수집부(120), 데이터필터링 및 축약부(130), 침입탐지부(140), 경고 및 보고부(150), 침입대응부(160)로 구성이 되어있다.

외부 또는 내부 네트워크(100)에서 감시대상 서버(110)가 있는 네트워크로 패킷이 발생하면, 데이터수집부(120)는 모든 트래픽을 수집하여 데이터 필터링 및 축약부(130)로 이를 전달한다.

데이터 필터링 및 축약부(130)는 방대한 양의 패킷(Row Data)들로부터 감시대상 서버(110)로 트래픽 만을 필터링하고, 침입탐지가 가능할 수 있도록 의미 있는 정보로의 전환 및 축약하고 침입탐지부(140)로 전달된다.

상기 침입탐지부(140)는 오용탐지부(141)와 비정상행위탐지부(142)로 구성된다. 상기 오용탐지부(141)는 시스템의 알려진 공격행위에 대한 특징 정보가 저장된 침입패턴 데이터베이스를 가지고 있으며, 발생한 이벤트(event)가 침입패턴 데이터베이스의 내용과 같으면, 침입으로 판정한다. 상기 비정상행위탐지부(142)는 정상적인 시스템 사용에 관한 프로파일과 시스템 상태를 저장한 프로파일 데이터베이스를 가지고 있으며, 발생한 이벤트가 프로파일 데이터베이스에 저장된 상태를 한계치 이상 벗어날 경우, 비정상행위로 판정한다.

발생한 이벤트가 침입탐지부(140)에서 침입으로 판정되면, 경고 및 보고부(150)에서 알람 등을 발생하여 관리자에게 알리고 관련 감사기록을 저장한다. 또한, 침입으로 판정된 이벤트에 대하여 침입대응부(160)에서는 관리자가 설정한 대응 행위에 따라 접속해제, 접근통제시스템의 환경 재설정 등 침입대응 기능을 수행한다.

이와 같이 구성된 종래의 침입탐지시스템에서 상기 오용탐지부(141)는 시스템 감사기록 정보에 대한 의존도가 높고, 상대적으로 구현 비용이 저렴하나 알려진 공격기법에 대한 탐지능력만을 가지고 있기 때문에, 최신 공격기법에 대한 계속적인 연구가 필요하며, 침입 시나리오를 추가시켜 주어야 하는 어려움이 있다. 오용탐지를 위하여 여러 방법들이 연구되어 왔는데 즉, 조건부 확률, 전문가시스템, 상태전이 분석, 패턴 매칭, CPN (Colored Petri-Net) 분석 등이 제안되었고, 복잡하고 다양한 침입을 어떻게 쉽게 표현할 것이며 이러한 방식을 사용하여 침입탐지율을 얼마나 높이느냐에 중점을 두고 있다. 대부분의 상용 침입탐지시스템들은 감사 이벤트(Audit Event)를 감사 데이터(Audit Trail)에서 감사 데이터의 순서, 데이터 패턴 등과 직접 찾을 수 있는 정보로 변환하여 해킹 데이터베이스와 비교하는 방식을 사용하고 있어 이를 통틀어 시그너쳐 분석(Signature Analysis)으로 부르기도 한다.

또한, 상기 비정상행위탐지부(142)는 정상적인 프로파일을 생성하는데 있어서 기존의 많은 데이터를 분석하여야 하기 때문에, 상대적으로 구현 비용이 크다. 비정상행위 탐지를 위하여 여러 방법들이 연구되어 왔는데 즉, 통계적 기법, 전문가 시스템, 데이터 마이닝(Data Mining), 은닉 마코브 모델(Hidden Markov Model), 컴퓨터 면역학, 신경망 등이 제안되었으며, 사용자들의 정상행위를 어떻게 표현하고 현재 발생되는 이벤트가 정상행위와 얼마나 차이가 나는지를 추론하는데 중점을 두고 있다. 이러한 비정상행위 탐지 기술은 오늘날 많은 연구의 주제가 되고 있으나 구현 비용이 너무 크고 오판율이 높아 상용에서는 사용하지 않는다. 상용제품에서 사용하는 비정상행위 탐지기술은 빈도수(frequencies), 분산(covariance), 평균(means) 등 통계치 프로파일을 유지하고 현재 발생되는 이벤트가 이들 한계치를 넘을 경우 침입으로 판정한다.

지금까지 많은 연구들은 오용탐지 방법이나 비정상행위 방법을 개선함으로써, 침입탐지율을 높이고 오판율을 줄이기 위하여 다양한 방법들이 연구되어 왔다. 오용탐지 기술과 비정상행위 기술의 혼합된 사용은 오용탐지는 알려진 공격으로 구성된 해킹 데이터베이스에 없는 침입은 탐지하지 못하며, 비정상행위는 정상행위를 벗어난 비정상 정도만을 표현할 뿐 침입을 정확히 지적하지 못한다는 문제점 때문에 두 방식간의 단점을 보완하기 위하여 병행 사용되고 있으나 두 방식을 혼합 사용하여 다른 형태의 침입을 분석하는 방식은 연구되고 있지 않다.

이처럼 침입탐지시스템에서 오용탐지와 비정상행위 탐지 기술을 중심으로 탐지 방법들이 연구되고 있으나, 오용 및 비정상행위탐지 이외의 다른 개념의 도입이나 다양한 침입탐지 방법들의 혼합된 사용으로 탐지율을 높이고 오판율을 줄이는 시도는 거의 이루어지지 않고 있다. 이러한 종래의 침입탐지시스템은 다음과 같은 문제점이 있다.

첫째, 기존의 침입탐지시스템은 오용탐지와 비정상행위탐지부 만으로 구성되어 있어서 기관의 보안 정책을 반영하기 힘들다. 대부분의 침입탐지시스템은 발생한 이벤트가 오용탐지부의 해킹 데이터베이스의 특정 내용과 같거나 비정상행위탐지부에서 정의한 한계치를 넘을 경우 침입임을 경고한다. 관리자는 단지 보안위반사건 데이터베이스와 일치성을 검사할 것인지 아닌지를 On/Off로 결정할 수 있으며, 한계치를 재조정할 수 있다. 종래의 침입탐지시스템은 기관의 보안정책과 관계없이 일률적인 적용만 가능하므로 기관이나 조직의 특성에 상관없이 동일한 동작형태를 갖는다.

둘째, 종래의 침입탐지시스템은 보안위반사건 데이터베이스에서 정의한 시그너쳐(Signature)와 일치하여야만 침입임을 판정한다. 시그너쳐의 연속으로 침입이 표현될 경우 일정 시간 진행되기 전까지는 침입으로 판정하지 않는다. 이로 인하여 침입이 시작되었음에도 불구하고 침입탐지시스템은 이벤트를 관찰 만하고 있으며 일정 시간이 경과한 후에야 침입임을 알아차림으로써 대응에 늦게된다.

셋째, 종래의 침입탐지시스템은 트래픽 중 감시대상으로의 트래픽만을 필터링하여 오용탐지부와 비정상행위탐지부로 전달된다. 전달된 패킷은 오용탐지부와 비정상행위탐지부에 해당 분석 모듈이 있을 경우 이를 모두 분석한다. 모든 해킹 데이터베이스의 검색을 방지하기 위하여 시스템 특성별 해킹 데이터베이스를 분리하거나 서비스별 해킹 데이터베이스를 분리하여 분산처리하며 어떤 시스템은 침입탐지시스템 설치시 필요한 데이터베이스만을 설치하여 시스템 부하를 줄일려고 한다. 그러나 해당 시스템과 서비스의 특성을 모두 고려하여 해킹 데이터베이스를 구성할 경우 설계의 어려움이 따르며, 불필요한 데이터베이스를 제거하였을 경우는 시스템의 서비스가 변동에 따라 다시 설치해야 하는 문제가 발생한다.

넷째, 종래의 침입탐지시스템은 서로 다른 공격으로 판단될 때 이를 각각 경고한다. 공격의 판정에 있어 여러 가지 시그너쳐들의 연관성을 보고 특정 공격으로 판정하고 있느나 판정된 공격들간의 연관성을 분석하여 새로운 공격으로 정의하지는 않음으로써 유사한 공격이 발생할 경우 불필요한 많은 알람을 발생시킨다.

발명이 이루고자 하는 기술적 과제

본 발명은 상기와 같은 문제점을 해결하기 위하여 안출된 것으로서 본 발명의 목적은 시스템 보안의 전통적 개념인 접근통제 기술을 침입탐지시스템에 도입하여 해킹 행위나 비정상행위는 아니지만 기관에서 정해놓은 보안정책을 위반할 경우에도 이를 탐지할 수 있는 침입탐지시스템을 제공하는데 있다.

본 발명의 다른 목적은 보안정책의 선적용 및 분산된 후공격탐지의 구조로 오용탐지부와 비정상행위 탐지부로 전달되는 감사데이터를 보안정책에서 필터링함으로써, 시스템의 부하를 줄이며 보안정책에 기반한 필터링 결과로 감시대상별 최적의 침입탐지 모듈만을 구성하여 효율적이고 빠른 침입탐지를 할 수 있는 침입탐지시스템을 제공하는데 있다.

본 발명의 또 다른 목적은 보안정책에 기반한 선탐지 기능과 즉각적인 대응 기능을 수행하고 재분석 기능을 통하여 세부 침입 정보를 후분석함으로써, 빠른 침입탐지 및 대응과 정확한 침입분석을 할 수 있는 침입탐지방법을 제공하는데 있다.

본 발명의 또 다른 목적은 오용분석부와 비정상행위탐지부에서 침입으로 판정된 침입데이터에 대하여 재분석하여 같은 공격형태에 대한 중복알람을 방지하고 연관성 있는 공격들을 하나의 공격형태로 표현함으로써, 불필요한 알람을 방지하는침입탐지방법을 제공하는데 있다.

발명의 구성 및 작용

상기와 같은 목적을 달성하기 위하여 본 발명은 외부 또는 내부 네트워크에서 감시대상인 서버가 있는 네트워크 패킷이 발생하면 모든 트래픽을 수집하는 데이터수집부와; 상기 데이터 수집부에서 수집된 데이터들을 침입탐지에 필요한 데이터만을 필터링하며 침입탐지가 가능할 수 있도록 의미 있는 정보로 전환 및 축약하는 데이터 필터링 및 축약부와; 상기 데이터 필터링 및 축약부에서 걸러진 데이터의 위반사항을 탐지 및 분석하는 침입탐지부와; 상기 침입탐지부에서 침입으로 분석되면 이에 대한 경고와 관련 감사기록을 남기는 경고 및 보고부와; 또한, 상기 침입탐지부에서 침입으로 분석되면 접속해재, 접근통제시스템의 환경 재설정 등의 정의된 대응행위를 수행하는 침입대응부를 포함하여 이루어진 것을 특징으로 한다.

또한, 상기 침입탐지부는 IP주소와 서비스 포트를 기반으로 감시대상 서버별 허용정책과 비허용정책 데이터베이스를 가지고 상기 데이터 필터링 및 축약부에서 수집된 데이터의 위반사항을 탐지하는 보안정책 위반탐지부와; 시스템의 알려진 공격 행위에 대한 특징 정보 데이터베이스를 가지고 있다가 해킹 데이터베이스와 같은 내용의 이벤트가 발생하면 침입을 알리는 오용탐지부와; 정상적인 시스템 사용에 관한 프로파일과 시스템 상태를 유지하고 있다가 이 프로파일에서 벗어나는 행위들을 탐지하는 비정상행위 탐지부와; 상기 보안정책 위반탐지부에서 위반된 패킷과 상기 오용탐지부 및 비정상행위 탐지부에서 침입으로 판정된 데이터에 대해 재분석하는 재분석부를 포함하여 이루어진 것을 특징으로 한다.

이하 본 발명의 바람직한 실시예를 첨부된 도면을 참조하여 상세히 설명한다.

도 2는 본 발명에 따른 보안정책에 기반한 다중 침입탐지시스템의 구성을 설명하기 위한 블록구성도이다.

여기에 도시된 바와 같이, 본 발명에 의한 침입탐지시스템은 데이터수집부(220), 데이터 필터링 및 축약부(230), 침입탐지부(240), 경고 및 보고부(250), 침입대응부(260)로 구성된다.

상기 데이터 수집부(220)는 외부 또는 내부 네트워크(200)에서 감시대상 서버(210)가 있는 네트워크로 모든 트래픽을 수집하고, 데이터 필터링 및 축약부(230)로 전달한다.

상기 데이터 필터링 및 축약부(230)는 감시대상 시스템으로 트래픽 만을 필터링하고 침입탐지에 필요한 데이터만을 추출하여 침입탐지가 가능할 수 있도록 의미 있는 정보로의 전환 및 축약한다.

상기 침입탐지부(240)은 보안정책위반탐지부(241), 오용탐지부(242), 비정상행위탐지부(243), 재분석부(244)로 구성된다. 상기 보안정책위반탐지부(241)는 접근통제 정책을 기반으로 감시대상 서버(210)별 허용정책과 거부정책를 가지고 위반 사항을 탐지한다. 위반된 패킷은 재분석부(244)에서 후분석 기능을 수행하며, 허가된 패킷은 오용탐지부(242)와 비정상행위탐지부(243)에서 분석된다. 상기 오용탐지부 (242)는 시스템의 알려진 공격행위에 대한 특징 정보가 저장된 침입패턴 데이터베이스를 가지고 있으며, 발생한 이벤트가 침입패턴 데이터베이스의 내용과 같으면 침입으로 판정한다. 상기 비정상행위탐지부(243)는 정상적인 시스템 사용에 관한 프로파일과 시스템 상태를 저장한 프로파일 데이터베이스를 가지고 있으며 발생한 이벤트가 프로파일 데이터베이스에 저장된 상태를 한계치 이상 벗어날 경우 비정상행위로 판정한다. 상기 재분석부(244)에서는 침입으로 판정된 데이터에 대하여 재분석하여 같은 공격형태에 대한 중복알람을 방지하고 연관성 있는 공격들을 하나의 공격형태로 표현함으로써, 불필요한 알람을 방지하는데 있다

상기 침입탐지부(240)에서 침입으로 판정되면 경고 및 보고부(250)에서 이에 대한 경고와 관련 감사기록을 남기고, 침입대응부(260)에서는 접속해제, 접근통제시스템의 환경 재설정 등 정의된 대응행위를 수행한다.

상기와 같이 구성된 본 발명의 상호동작은 도 3에 도시된 바와 같이, 외부 또는 내부 네트워크(300)에서 감시대상 서버(301)가 있는 네트워크로 패킷이 발생하면 데이터 수집부(302)는 모든 트래픽을 수집하여 데이터 필터링 및 축약부(303)로 이를 전달한다.

상기 데이터 필터링 및 축약부(303)는 방대한 양의 패킷(Row Data)들로부터 감시대상 목록 저장부(312)의 감시대상 목록에 기반하여 트래픽을 필터링하고, 침입탐지가 가능할 수 있도록 의미 있는 정보로의 전환 및 축약하고 보안정책위반탐지부(304)로 전달한다.

상기 보안정책위반탐지부(304)는 감시대상별 보안정책 저장부(313)의 감시대상별 보안정책 목록에 기반하여 기관의 보안 정책을 위반하였는지 판정한다. 허용된 패킷은 오용탐지부(305)와 비정상행위탐지부(306)로 전달되며, 위반된 패킷은 결과 조정 및 감사데이터 생성부(308)를 거쳐 재분석부(307)에서 분석되고 즉각적인 대응과 보고를 위하여 침입대응부(309)와 경고 및 보고부(310)로 전달된다.

상기 오용탐지부(305)는 보안정책위반탐지부(304)에서 허용된 패킷만을 분석하며 침입패턴 저장부(314)의 침입패턴 데이터베이스와 비교하여 일치하는 것이 있으면 침입으로 판정한다. 침입으로 판정된 데이터는 결과 조정 및 감사데이터 생성부(308)를 거쳐 재분석부(307)에서 분석되고 즉각적인 대응과 보고를 위하여 침입대응부(309)와 경고 및 보고부(310)로 전달된다.

상기 비정상행위탐지부(306)는 보안정책위반탐지부(304)에서 허용된 패킷만을 분석하며 프로파일 저장부(315)의 프로파일 데이터베이스와 비교하여 한계치를 넘으면 비정상행위로 판정한다. 침입으로 판정된 데이터는 결과 조정 및 감사데이터 생성부(308)를 거쳐 재분석부(307)에서 분석되고, 즉각적인 대응과 보고를 위하여 침입대응부(309)와 경고 및 보고부(310)로 전달된다.

상기 결과 조정 및 감사데이터 생성부(308)는 보안정책위반탐지부(304), 오용탐지부(305), 비정상행위탐지부(306)로부터 침입탐지 결과를 전달받고 재분석부(307), 침입대응부(309), 경고 및 보고부(310) 등에서 처리하기 알맞은 형태로 데이터를 변형하고 축약된 감사데이터를 생성하며, 처음 발견된 공격에 대하여 빠른 대응을 위한 침입대응부(309), 경고 및 보고부(310)로 우선 전달하며 연속적인 공격 등에 대하여 재분석부(307)로 전달하여 결과를 침입대응부(309), 경고 및 보고부(310)로 다시 전달한다.

상기 재분석부(306)는 보안정책위반탐지부(304)에서 거부으로 판정된 이벤트에 대하여 재분석패턴 데이터베이스와 비교하여 세부 침입 정보를 분석하고, 상기 오용탐지부(305)와 비정상행위탐지부(306)에서 침입으로 판정된 이벤트에 대하여 같은 공격일 경우 중복알람으로 인식하고, 일정 시간 간격 또는 끝난 시간과 회수 등의 정보를 제공하며, 상기 오용탐지부(305)와 비정상행위탐지부(306)에서 여러 이벤트가 침입으로 판정되고 서로 다른 정보일 경우, 연관성 있는 공격에 대하여 재분석 패턴 데이터베이스와 비교하여 하나의 공격형태로 표현하거나 다중 공격을 탐지한다.

상기 침입대응부(309)는 결과조정 및 감사데이터 생성부(308)로부터 침입 행위를 전달받으면, 침입 대응 규칙 저장부(317)의 침입대응 규칙에 기반하여 해당되는 대응 행위를 수행한다.

상기 경고 및 보고부(310)는 결과조정 및 감사데이터 생성부(308)로부터 침입 행위를 전달받으면, 관리자에게 이를 통보하기 위하여 알람을 발생시키고 보안관리부(311)로 보고한다.

상기 보안관리부(311)는 침입탐지시스템에서 사용되는 모든 데이터를 관리한다.

도 4는 본 발명에 따른 데이터 필터링 및 축약부와 보안정책위반탐지부를 설명하기 위한 흐름도이다.

여기에 도시된 바와 같이, 데이터 수집부(S400)에서 수집된 패킷은 데이터 필터링 및 축약부(S410)에서 감시대상 목록(S413)을 참조하여 감시대상 트래픽인지 비교한다(S412). 만약, 감시대상 트래픽이 아니면, 패킷을 드롭(drop)시키고(S411), 그렇지 않고, 감시대상 트래픽이면, 이를 보안정책위반탐지부(S420)로 전달한다.

상기 보안정책위반탐지부(S420)는 먼저, 감시대상에 대한 보안정책 검색 데이터베이스를 검색(S421)하고, 보안정책이 허용정책인지 거부정책인지 비교한다(S422). 상기 감시대상별 보안정책은 허용목록(S425)과 거부목록(S426)으로 구성되어 있다.

만약, 허용정책일 경우 허용목록(S425)을 참조하여 허용된 서비스인지 검사한다(S423). 허용된 서비스이면, 오용탐지부(S440)와 비정상행위탐지부(S450)로 패킷을 전달하고, 그렇지 않고 허용된 서비스가 아니면, 결과조정 및 감사데이터 생성부(S430)를 통하여 침입대응부(S432)와 재분석부(S434)로 전달된다.

만약, 거부정책일 경우 거부목록(S426)를 참조하여 거부된 서비스인지 검사한다(S424). 거부된 서비스가 아니면, 오용탐지부(S440)와 비정상행위탐지부(S450)로 패킷을 전달하고, 거부된 서비스이면, 결과조정 및 감사데이터 생성부(S430)를 통하여 침입대응부(S432)와 재분석부(S434)로 전달된다.

도 5는 본 발명에 따른 오용탐지부를 설명하기 위한 흐름도이다.

여기에 도시된 바와 같이, 상기 보안정책위반탐지부(S420)에서 허용된 데이터만이 오용탐지부(S510)로 전달되며, 상기 오용탐지부(S510)에서는 먼저, 네트워크 프로토콜 관련 시그너쳐(Signature)를 추출한다(S511). 다음으로, 침입패턴 데이터베이스(S518)와 비교하여 네트워크 프로토콜 공격인지 판단한다(S512). 만약, 네트워크 프로토콜 공격이면, 결과조정 및 감사데이터 생성부(S430)를 통하여 침입대응부(S432)와 재분석부(S434)로 전달된다. 그렇지 않고 네트워크 프로토콜 공격 이 아니면, 응용 서비스를 식별하고 해당 탐지모듈로 데이터를 전달한다(S513). 개별 응용서비스 탐지모듈에서는 먼저, 응용서비스별 시그너쳐를 추출(S514)하고, 침입탐지 범위를 설정한다(S515). 침입패턴 데이터베이스(S518)와 비교하여 응용서비스 공격인지를 판단한다(S516). 만약, 응용서비스 공격이면, 결과조정 및 감사데이터 생성부(S430)를 통하여 침입대응부(S432)와 재분석부(S434)로 전달되고, 그렇지 않고 응용서비스 공격이 아니면, 종료한다(S517).

도 6은 본 발명에 따른 비정상행위탐지부를 설명하기 위한 흐름도이다.

여기에 도시된 바와 같이, 상기 보안정책 위반탐지부(S420)에서 허용된 데이터만이 비정상행위탐지부(S450)로 전달되며, 상기 비정상행위탐지부(S450)에서는 먼저, 패킷 데이터로부터 필요한 상태값을 추출(S611)하고, 전체 네트워크에 대한 상태값을 계산한다(S612). 전체 네트워크에 대한 상태값과 프로파일 데이터베이스(S617)를 비교하여 비정상인지 판단한다(S613). 만약, 비정상 트래픽일 경우, 결과조정 및 감사데이터 생성부(S430)를 통하여 침입대응부(S432)와 재분석부(S434)로 이를 전달되고, 정상 트래픽일 경우, 감시대상별/서비스별 네트워크 상태값을 계산한다(S614). 상기 감시대상별/서비스별 네트워크 상태값과 프로파일 데이터베이스(S617)를 비교하여 비정상인지 비교한다(S615). 비정상 트래픽일 경우, 결과조정 및 감사데이터 생성부(S430)를 통하여 침입대응부(S432)와 재분석부(S434)로 전달되고 정상일 경우, 종료한다(S616).

도 7은 본 발명에 따른 결과조정 및 감사데이터 생성부를 설명하기 위한 흐름도이다.

여기에 도시된 바와 같이, 보안정책위반탐지부(S420), 오용탐지부(S440), 비정상행위탐지부(S450)에서 침입으로 판정된 데이터나 재분석부(S740)에서 재분석된 결과는 결과조정 및 감사데이터 생성부(S630)로 전달된다. 상기 결과조정 및 감사데이터 생성부(S630)에서는 침입으로 판정된 데이터로부터 재분석부(S740), 경고 및 보고부(S650) 및 침입대응부(S432)에서 필요한 정보로 구성하여 감사데이터를 생성한다(S631). 다음으로 공격형태 및 탐지부를 식별(S632)하고, 재분석된 결과인지 다른 침입탐지부에서 침입으로 판정된 결과인지 판단한다(S633). 만약, 재분석된 결과이면, 침입대응이 필요한지를 식별(S635)하고, 대응이 필요 없으면 경고 및 보고부(S650)로 전달되고, 대응이 필요하면 경고 및 보고부(S650)와 침입대응부(S432)로 전달된다.

그렇지 않고, 재분석 결과가 아니면, 첫번째 탐지된 공격인지를 판단한다(S634). 첫번째 탐지된 공격이면, 침입대응이 필요한지를 식별(S635)하는 단계로 전달되고, 재분석을 위하여 재분석부(S740)로도 전달된다. 공격의 주체 및 객체 정보가 유사하고 첫번째 공격이 아닐 경우 중복알람방지, 유사 공격 및 다중 공격을 분석하기 위하여 재분석부(S740)로 전달된다.

도 8은 본 발명에 따른 재분석부를 설명하기 위한 흐름도이다.

여기에 도시된 바와 같이, 보안정책위반탐지부(S420), 오용탐지부(S44) 및 비정상행위탐지부(S450)에서 침입으로 판정된 데이터는 결과조정 및 감사데이터 생성부(S630)를 거쳐 재분석부(S740)로 전달된다. 상기 재분석부(S740)에서는 공격 정보를 추출(S711)하고, 주체와 객체의 유사성을 비교한다(S712). 만약, 유사한 주체 또는 객체 정보가 없으면, 첫번째 공격으로 인식하고 탐지정보 임시저장소(S716)에 이를 저장한다. 그렇지 않고, 유사한 주체 및 객체 정보가 있으면, 같은 공격인지 비교한다(S713). 만약, 같은 공격일 경우, 탐지정보 임시저장소(S716)에 관련 정보를 수정한다. 같은 공격이 아닐 경우, 재분석 패턴 데이터베이스(S717)와 비교하여 유사공격, 다중공격 등 새로운 공격 형태를 지정할 수 있는지 비교한다(S714). 새로 정의할 수 없는 공격이면, 결과 조정 및 감사데이터 생성부(S630)로 전달되고, 재분석 패턴 데이터베이스(S717)와 같은 패턴이 있을 경우 새로운 형태의 공격을 보고(S715)하고, 결과조정 및 감사데이터 생성부(S630)에 전달한다. 상기 탐지정보임시저장소(S716)는 새로운 정보를 받아들이고 사용되지 않는 오래된 정보를 삭제하기 위해 주기적으로 탐지정보 검사하고 관리한다(S718). 타임아웃(Timeout) 또는 관리자가 정의한 일정 시간 간격을 점검(S719)하고 수정된 데이터를 결과조정 및 감사데이터 생성부(S630)에 전달한다.

도 9는 본 발명에 따른 다른 실시예로서, 결과조정 및 감사데이터 생성부를 사용하지 않고 보안정책위반탐지부, 오용탐지부 및 비정상행위탐지부와 재분석부에서 이 기능을 부분적으로 나누어 수행하는 것을 나타내는 도면이다.

여기에 도시된 바와 같이, 외부 또는 내부 네트워크(900)에서 감시대상인 서버(901)가 있는 네트워크로 패킷이 발생하면 데이터 수집부(902)는 모든 트래픽을 수집하여 데이터 필터링 및 축약부(903)로 이를 전달한다.

데이터 필터링 및 축약부(903)는 방대한 양의 패킷(Row Data)들로부터 감시대상 목록 저장부(911)의 감시대상 목록에 기반하여 트래픽을 필터링하고, 침입탐지가 가능할 수 있도록 의미 있는 정보로의 전환 및 축약하고 보안정책탐지부(904)로 전달한다.

상기 보안정책위반탐지부(904)는 감시대상별 보안정책 저장부(312)의 감시대상별 보안정책 목록에 기반하여 기관의 보안 정책을 위반하였는지 판정한다. 허용된 패킷은 오용탐지부(905)와 비정상행위탐지부(906)로 전달되고, 위반된 패킷은 즉각적인 대응과 보고를 위하여 침입대응부(908)과 경고 및 보고부(909)로 전달되며 세부 침입 정보를 분석하기 위하여 재분석부(907)로 전달된다.

상기 오용탐지부(905)는 보안정책위반탐지부(904)에서 허용된 패킷만을 분석하며 침입패턴 저장부(913)의 침입패턴 데이터베이스와 비교하여 일치하는 것이 있으면 침입으로 판정한다. 침입으로 판정된 즉각적인 대응과 보고를 위하여 침입대응부(908)과 경고 및 보고부(909)로 전달되며, 중복알람 방지, 유사 공격 및 다중 공격을 분석하기 위하여 재분석부(907)로 전달된다.

상기 비정상행위탐지부(906)는 보안정책위반탐지부(304)에서 허용된 패킷만을 분석하며 프로파일 저장부(914)의 프로파일 데이터베이스와 비교하여 한계치를 넘으면 비정상행위로 판정한다. 침입으로 판정된 데이터는 즉각적인 대응과 보고를 위하여 침입대응부(908)과 경고 및 보고부(909)로 전달되며, 중복알람 방지, 유사 공격 및 다중 공격을 분석하기 위하여 재분석부(907)로 전달된다.

상기 재분석부(907)는 보안정책위반탐지부(904)에서 거부으로 판정된 이벤트에 대하여 재분석패턴 데이터베이스와 비교하여 세부 침입 정보를 분석하고, 오용탐지부(905)와 비정상행위탐지부(906)에서 침입으로 판정된 이벤트에 대하여 같은 공격일 경우 중복알람으로 인식하고 일정 시간 간격 또는 끝난 시간과 회수 등의 정보를 제공하며, 오용탐지부(905)와 비정상행위탐지부(906)에서 여러 이벤트가 침입으로 판정되고 서로 다른 정보일 경우, 연관성 있는 공격에 대하여 재분석 패턴데이터베이스와 비교하여 하나의 공격형태로 표현하거나 다중 공격을 탐지한다.

상기 침입대응부(908)는 각 침입탐지부에서 침입 행위를 전달받으면 침입 대응 규칙 저장부(916)의 침입대응 규칙에 기반하여 해당되는 대응 행위를 수행한다.

상기 경고 및 보고부(909)는 각 침입탐지부에서 침입 행위를 전달받으면 관리자에게 이를 통보하기 위하여 알람을 발생시키고 보안관리부(910)로 보고한다.

상기 보안관리부(910)는 침입탐지시스템에서 사용되는 모든 데이터를 관리한다.

또 다른 실시예로서 다음과 같이 재분석부를 사용하지 않는 경우와 보안정책위반탐지부를 사용하지 않는 경우도 있을 수 있다.

먼저, 재석부를 사용하지 않고 오용탐지부 및 비정상행위탐지부가 보안정책위반탐지부와 결합한 예로 상기 보안정책위반탐지부의 독립적 사용 즉, 보안정책위반탐지부, 오용탐지부, 비정상행위탐지부를 병렬로 사용할 수도 있다.

또한, 보안정책위반탐지부를 사용하지 않고, 오용탐지부 및 비정상행위탐지부가 재분석부와 결합하여 이용할 수도 있다.

발명의 효과

따라서, 상기한 바와 같이 본 발명은 침입차단시스템 등에서 사용하는 접근통제 기술을 침입탐지시스템에 적용한 것으로, 시스템이나 네트워크에 대하여 기관의 보안정책 수립하고 침입탐지시스템에 반영하도록 함으로써, 오용탐지부나 비정상행위 탐지부에서 탐지하지 못하는 다양한 보안위반 사항들을 탐지할 수 있고, 최근 해킹 도구들이 패킷을 암호화하는 반면 기존 침입탐지시스템은 암호화된 패킷을 분석하지 못한다. 그러나 대부분의 백도어가 기관에서 허용하지 않는 서비스를 사용하므로 패킷을 분석하지 않더라도 허가되지 않은 패킷임을 탐지할 수 있는 이점이 있다.

또한, 본 발명은 보안정책 위반탐지부에서 위반으로 탐지된 이벤트에 대하여 재분석 기능을 수행함으로써, 선탐지 및 대응, 후분석을 가능하게 하며 오판율을 줄여줄 수 있는 이점이 있다??예를 들면, 포트 스캔의 경우 기존 침입탐지시스템에서는 한계 포트 이상에 대하여 접속 요구를 하였을 경우 이를 포트 스캔으로 탐지하고 대응 행동을 수행한다. 그러나, 정당한 시스템 관리자가 네트워크를 점검하기 위하여 여러 포트를 점검하였을 경우 이 또한 침입으로 판정한다. 본 발명에서는 허가된 관리자가 허가된 포트를 점검하였을 경우 이를 침입으로 판정하지 않으며 허가되지 않은 사용자가 서비스의 이용을 시도할 때 침입으로 간주한다. 허가되지 않은 사용자가 하나의 서비스 포트에 접근할 때 보안정책 위반임을 탐지하고 대응 행동을 수행하므로 여러 개의 포트가 진행되는 동안 관찰만 하는 기존 침입탐지시스템보다 빠른 동작 구조를 갖는다. 기존 침입탐지 시스템과 같이 보다 세부적인 침입 관련 정보를 관리자에게 제공하기 위하여 재분석부에서 대응 행동 수행 동안 패킷을 분석하여 포트 스캔임을 알려준다.

또한, 본 발명은 보안정책 위반탐지부에서 허용된 패킷만이 오용탐지부와 비정상행위 탐지부로 전달되므로 많은 패킷이 필터링되며 보안정책에서 허용된 분석 모듈만이 오용탐지부와 비정상행위탐지부에서 동작하므로 침입탐지시스템의 부하를 줄여준다. 그러므로 오용탐지부와 비정상행위 탐지부는 기존 침입탐지시스템 보다 빠르게 동작할 수 있는 이점이 있다.

또한, 본 발명은 오용분석부와 비정상행위탐지부에서 침입으로 판정된 데이터에 대하여 재분석함으로써, 같은 공격형태에 대한 중복알람을 방지하고 연관성 있는 다른 공격형태에 대한 새로운 공격형태의 표현으로 불필요한 알람을 방지할 수 있는 이점이 있다.

(57) 청구의 범위

청구항 1.

외부 또는 내부 네트워크에서 감시 대상이 있는 네트워크간의 트래픽을 분석하고 침입을 탐지하는 침입탐지시스템에 있어서,

감시대상 서버가 제공하는 시스템 사용내역 또는 감시대상 서버로부터 네트워크 패킷 등의 데이터를 수집하는 데이터수집부와;

침입탐지에 필요한 데이터만을 필터링하고 침입탐지가 가능할 수 있도록 의미 있는 정보로 전환 및 축약하는 데이터 필터링 및 축약부와;

상기 데이터 필터링 및 축약부에서 수집된 데이터의 위반사항을 탐지 및 분석하는 IP주소와 서비스 포트를 기반으로 감시대상 서버별 허용정책과 비허용정책 데이터베이스를 가지고 상기 데이터 수집 및 축약부에서 수집된 데이터의 위반사항을 탐지하는 보안정책위반탐지부와, 시스템으 알려진 공격 행위에 대한 특징 정보 데이터베이스를 가지고 있다가 해킹 데이터베이스와 같은 내용의 이벤트가 발생하면 침입을 알리는 오용탐지부와, 정상적인 시스템 사용에 관한 프로파일과 시스템 상태를 유지하고 있다가 이 프로파일에서 벗어나는 행위들을 탐지하는 비정상행위 탐지부와, 상기 보안정책위반탐지부에서 위반된 패킷과 상기 오용탐지부 및 비정상행위 탐지부에서 침입으로 판정된 데이터에 대해 재분석하는 재분석부를 포함하여 구성되어진 침입탐지부와;

상기 침입탐지부에서 침입으로 분석되면 이에 대한 경고와 관련 감사기록을 남기는 경고 및 보고부와;

상기 침입탐지부에서 침입으로 분석되면 접속해재, 접근통제시스템의 환경 재설정 등의 정의된 대응행위를 수행하는 침입대응부를 포함하여 이루어진 것을 특징으로 하는 다양한 침입탐지모델을 사용하는 침입탐지시스템.

청구항 2.

제 1항에 있어서, 상기 보안정책위반탐지부, 오용탐지부, 비정상행위탐지부로부터 침입탐지 결과를 전달받고, 상기 재분석부, 침입대응부, 경고 및 보고부 등에서 처리하기 알맞은 형태로 데이터를 변형하고 축약된 감사데이터를 생성하는 결과 조정 및 감사데이터 생성부를 더 포함하여 이루어진 것을 특징으로 하는 다양한 침입탐지모델을 사용하는 침입탐지시스템.

청구항 3.

외부 또는 내부 네트워크에서 감시 대상이 있는 네트워크간의 트래픽을 분석하고 침입을 탐지하는 침입탐지방법에 있어서,

데이터 수집부에서 수집된 패킷은 데이터 필터링 및 축약부에서 감시대상 목록을 참조하여 감시대상 트래픽인지 비교하는 제 1판단 단계와,

상기 제 1판단 단계에서 감시대상 트래픽이 아니면, 패킷을 드롭시키는 단계와,

상기 제 1판단 단계에서 감시대상 트래픽이면, 감시대상에 대한 보안정책 검색 데이터베이스를 검색하는 검색단계와,

상기 검색단계에서 검색된 데이터가 허용정책인지 거부정책인지 비교하는 제 2판단 단계와,

상기 제 2판단 단계에서 허용정책일 경우 허용목록을 참조하여 허용된 서비스인지 검사하는 제 3판단 단계와,

상기 제 3판단 단계에서 허용된 서비스이면, 오용탐지부와 비정상행위탐지부로 패킷을 전달하는 단계와,

상기 제 3판단 단계에서 허용된 서비스가 아니면, 결과조정 및 감사데이터 생성부를 통하여 침입대응부와 재분석부로 전달되는 단계와,

상기 제 2판단 단계에서 거부정책일 경우 거부목록를 참조하여 거부된 서비스인지 검사하는 제 4판단 단계와,

상기 제 4판단 단계에서 거부된 서비스가 아니면, 오용탐지부와 비정상행위탐지부로 패킷을 전달하는 단계와,

상기 제 4판단 단계에서 거부된 서비스이면, 결과조정 및 감사데이터 생성부를 통하여 침입대응부와 재분석부로 전달되는 단계를 포함하는 것을 특징으로 하는 다양한 침입탐지모델을 사용하는 침입탐지방법.

청구항 4.

제 3항에 있어서, 상기 오용탐지부에서는 먼저, 네트워크 프로토콜 관련 시그너쳐를 추출하는 제 1추출단계와,

상기 제 1추출단계에서 추출된 시그너쳐와 침입패턴 데이터베이스를 비교하여 네트워크 프로토콜 공격인지를 판단하는 제 5판단 단계와,

상기 제 5판단 단계에서 네트워크 프로토콜 공격이면, 결과조정 및 감사데이터 생성부를 통하여 침입대응부와 재분석부로 전달되는 단계와,

상기 제 5판단 단계에서 네트워크 프로토콜 공격이 아니면, 응용 서비스를 식별하고 해당 탐지모듈로 데이터를 분배하는 분배단계와,

상기 분배단계에서 분배된 데이터를 응용서비스별로 시그너쳐를 추출하는 제 2추출단계와,

상기 제 2추출단계에서 추출된 데이터로 침입탐지 범위를 설정하는 설정단계와,

상기 설정단계에서 설정된 데이터와 침입패턴 데이터베이스와 비교하여 응용서비스 공격인가를 판단하는 제 6판단 단계와,

상기 제 6판단 단계에서 응용서비스 공격이면, 결과조정 및 감사데이터 생성부를 통하여 침입대응부와 재분석부로 전달되는 단계와,

상기 제 6판단 단계에서 응용서비스 공격이 아니면, 종료하는 단계를 포함하는 것을 특징으로 하는 다양한 침입탐지모델을 사용하는 침입탐지방법.

청구항 5.

제 3항에 있어서, 상기 비정상행위탐지부에서는 먼저, 패킷 데이터로부터 필요한 상태값을 추출하는 변환단계와,

상기 변환단계에서 변환된 데이터로 전체 네트워크에 대한 상태값을 계산하는 제 1계산단계와,

상기 전체 네트워크에 대한 상태값과 프로파일 데이터베이스를 비교하여 비정상인지 비교하는 제 7판단 단계와,

상기 제 7판단 단계에서 비정상 트래픽일 경우, 결과조정 및 감사데이터 생성부를 통하여 침입대응부와 재분석부로 전달되는 단계와,

상기 제 7판단 단계에서 정상 트래픽일 경우, 감시대상별/서비스별 네트워크 상태값을 계산하는 제 2계산단계와,

상기 감시대상별/서비스별 네트워크 상태값과 프로파일 데이터베이스를 비교하여 비정상인지 비교하는 제 8판단 단계와,

상기 제 8판단 단계에서 비정상 트래픽일 경우, 결과조정 및 감사데이터 생성부를 통하여 침입대응부와 재분석부로 전달되는 단계와,

상기 제 8판단 단계에서 정상 트래픽일 경우, 종료하는 단계를 포함하는 것을 특징으로 하는 다양한 침입탐지모델을 사용하는 침입탐지방법.

청구항 6.

제 3항에 있어서, 상기 결과조정 및 감사데이터 생성부에서는 침입으로 판정된 데이터로부터 재분석부, 경고 및 보고부 및 침입대응부에서 필요한 정보로 구성하여 감사데이터를 생성하는 생성단계와,

상기 생성단계에서 생성된 감사데이터를 공격형태 및 탐지부로 식별하는 식별단계와,

상기 식별단계에서 식별된 데이터를 재분석된 결과인지 다른 침입탐지부에서 침입으로 판정된 결과인지 판단하는 제 9판단 단계와,

상기 제 9판단 단계에서 재분석된 결과가 아니면, 첫번째 탐지된 공격인지를 판단하는 제 10판단 단계와,

상기 제 10판단 단계에서 첫번째 탐지된 공격이면, 침입대응이 필요한지를 식별하는 제 11단계와,

상기 제 11판단 단계에서 침입대응이 필요하면 경고 및 보고부와 침입대응부로 전달되는 단계와,

상기 제 11판단 단계에서 침입대응이 필요 없으면 경고 및 보고부로 전달되는 단계와,

상기 제 10판단 단계에서 첫번째 탐지된 공격이 아니면, 중복알람방지, 유사 공격 및 다중 공격을 분석하기 위하여 재분석부로 전달되는 단계와,

상기 제 9판단 단계에서 재분석된 결과이면, 침입대응이 필요한지를 식별하는 제 11판단 단계로 이동하는 단계를 포함하는 것을 특징으로 하는 다양한 침입탐지모델을 사용하는 침입탐지방법.

청구항 7.

제 3항에 있어서, 상기 재분석부에서는 공격 정보를 추출하는 제 3추출단계와,

상기 제 3추출단계에서 추출된 데이터의 주체와 객체의 유사성을 비교하는 제 12판단 단계와,

상기 제 12판단 단계에서 유사한 주체 또는 객체 정보가 없으면, 첫번째 공격으로 인식하고 탐지정보 임시저장소에 이를 저장하는 단계와,

상기 제 12판단 단계에서 유사한 주체 및 객체 정보가 있으면, 같은 공격인지 비교하는 제 13판단 단계와,

상기 제13판단 단계에서 같은 공격일 경우, 탐지정보 임시저장소에 관련 정보를 수정하는 단계와,

상기 제 13판단 단계에서 같은 공격이 아닐 경우, 재분석 패턴 데이터베이스와 비교하여 유사공격, 다중공격 등 새로운 공격 형태를 지정할 수 있는지 비교하는 제 14판단 단계와,

상기 제 14판단 단계에서 새로 정의할 수 없는 공격이면, 결과 조정 및 감사데이터 생성부로 전달되는 단계와,

상기 제 14판단 단계에서 재분석 패턴 데이터베이스와 같은 패턴이 있을 경우, 새로운 형태의 공격을 보고하고, 결과조정 및 감사데이터 생성부에 전달하는 단계를 포함하는 것을 특징으로 하는 다양한 침입탐지모델을 사용하는 침입탐지방법.

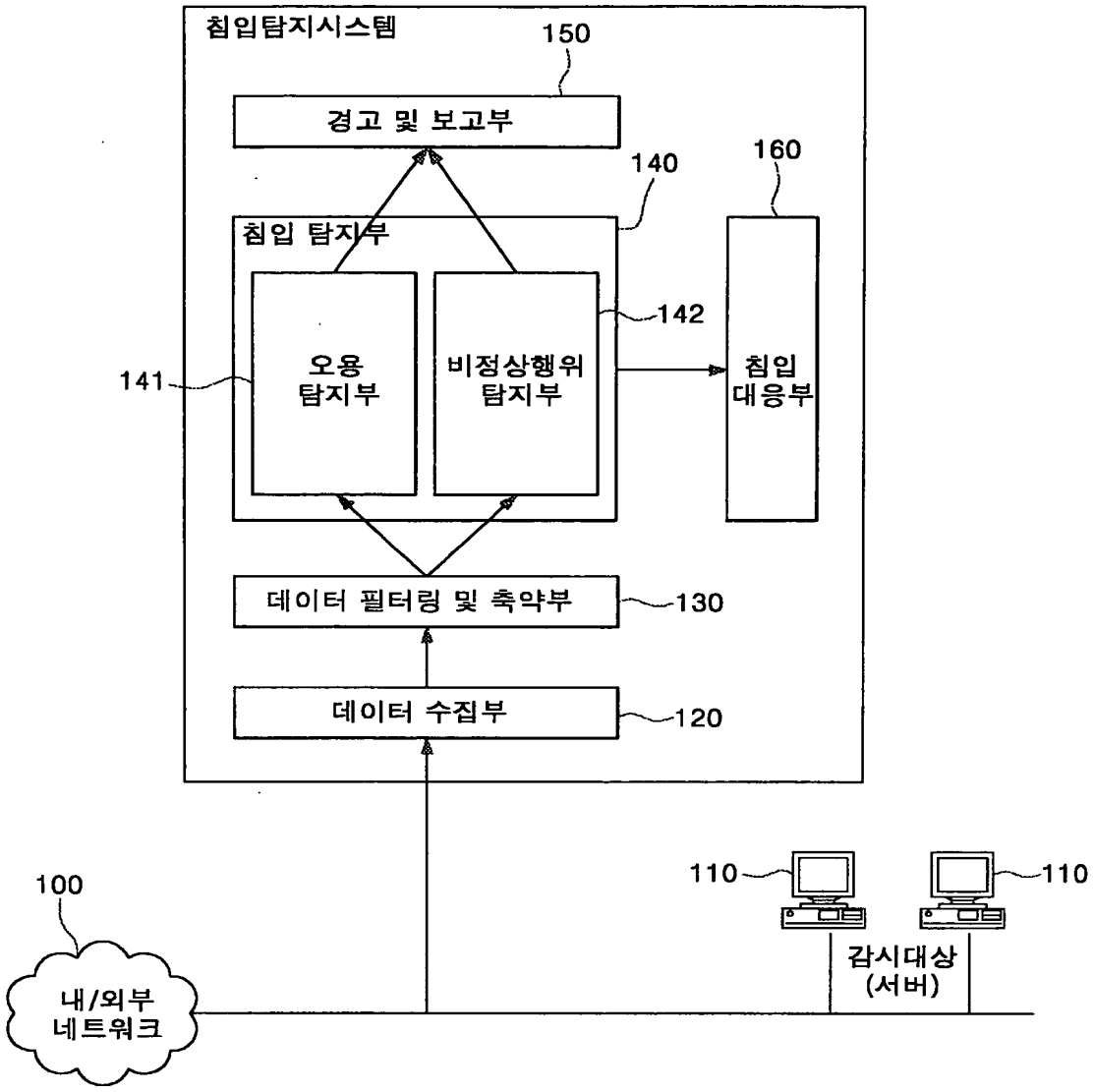
청구항 8.

제 7항에 있어서, 상기 탐지정보임시저장소는 새로운 정보를 받아들이고 사용되지 않는 오래된 정보를 삭제하기 위해 주기적으로 탐지정보 검사하고 관리하는 관리단계와,

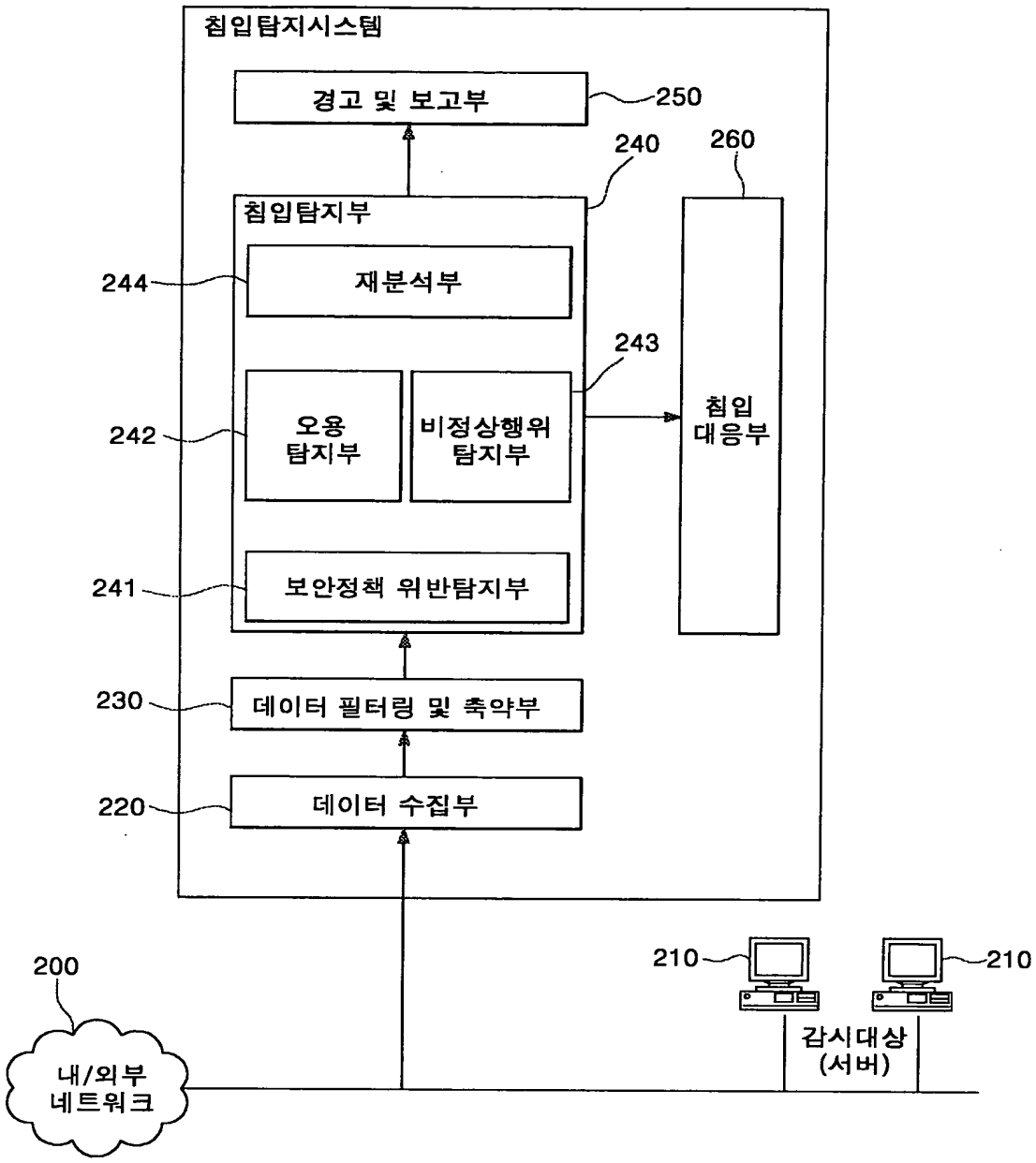
상기 관리단계에서 검사한 데이터를 타임아웃 또는 관리자가 정의한 일정 시간 간격을 점검하고 수정된 데이터를 결과조정 및 감사데이터 생성부에 전달하는 단계를 포함하는 것을 특징으로 하는 다양한 침입탐지모델을 사용하는 침입탐지방법.

도면

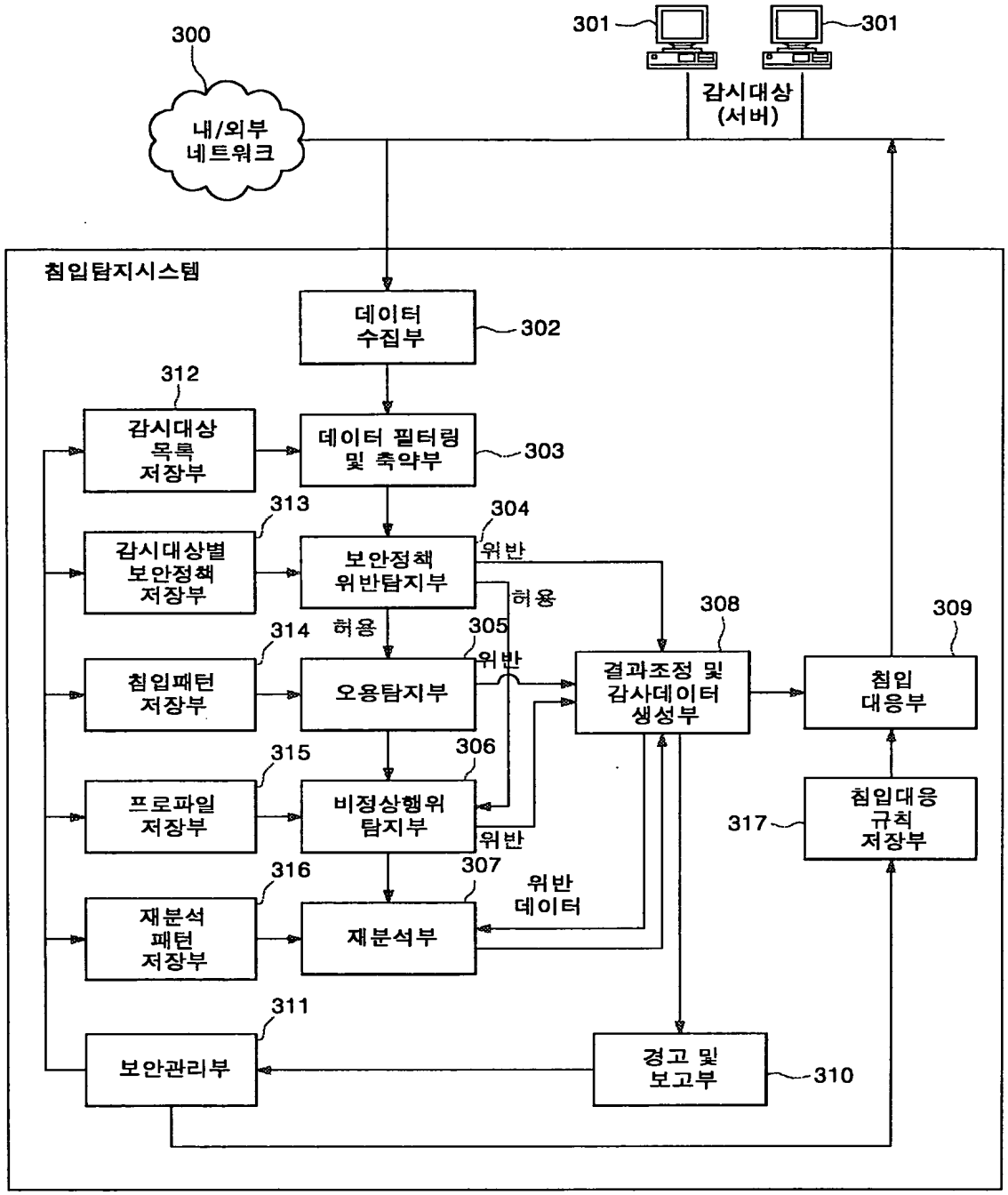
도면 1


침입탐지시스템
150
경고 및 보고부
140
160
침입 탐지부
142
141
오용
탐지부
비정상행위
탐지부
침입
대응부
데이터 필터링 및 축약부
130
데이터 수집부
120
100
내/외부
네트워크
110
110
감시대상
(서버)

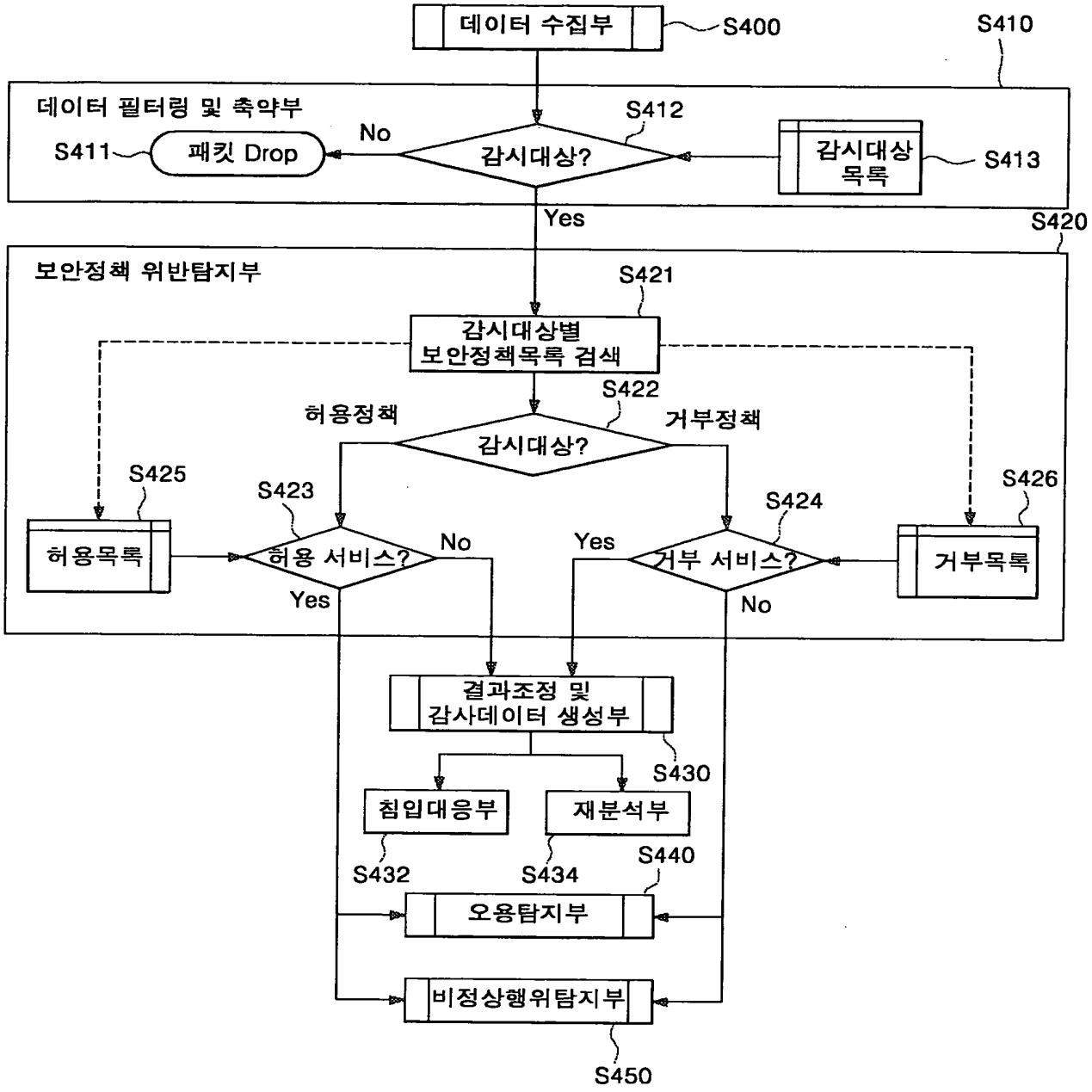
도면 2


침입탐지시스템
경고 및 보고부
250
240
260
침입탐지부
244
재분석부
243
242
오용
탐지부
비정상행위
탐지부
침입
대응부
241
보안정책 위반탐지부
230
데이터 필터링 및 축약부
220
데이터 수집부
200
210
210
내/외부
네트워크
감시대상
(서버)

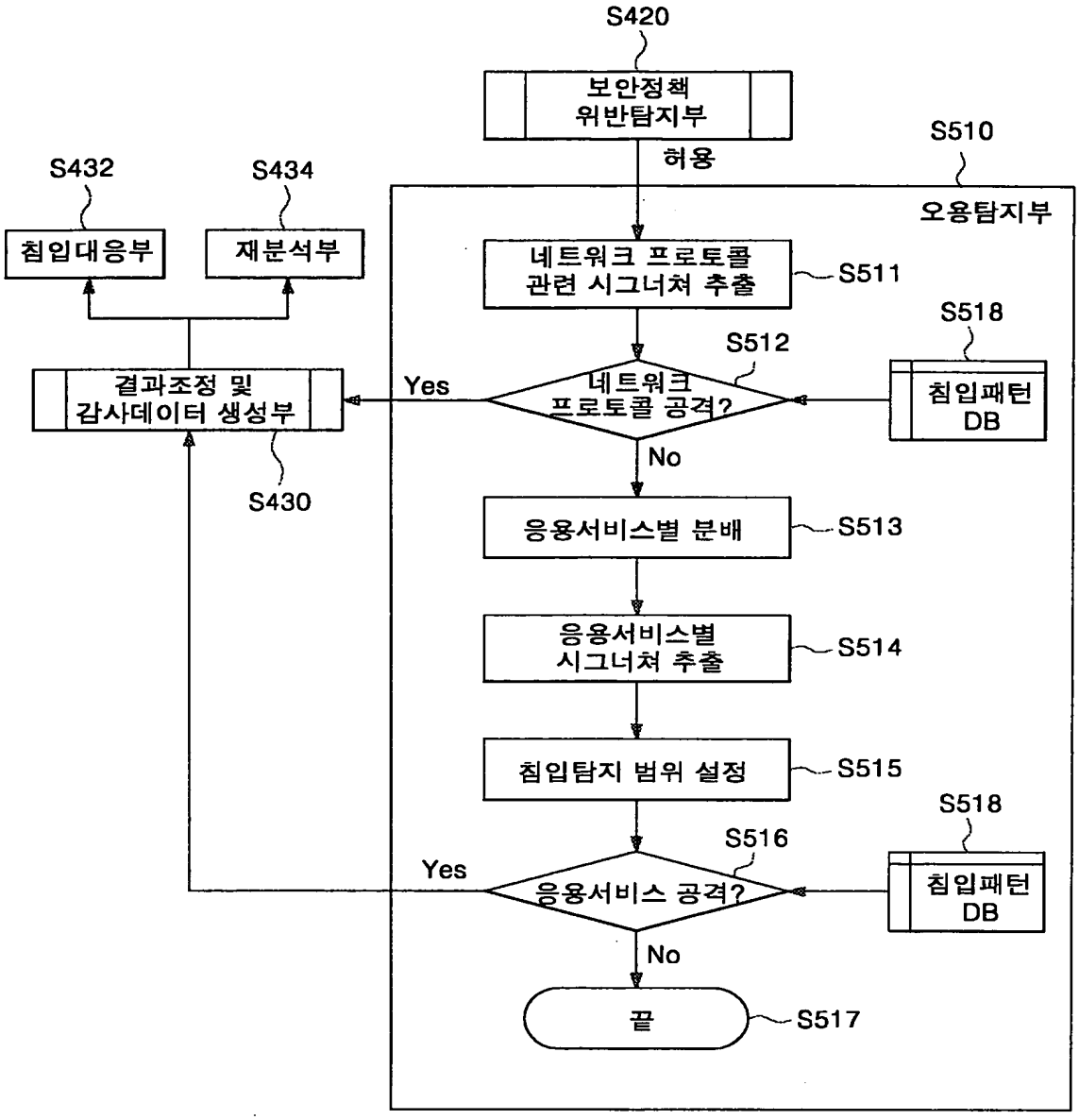
도면 3


300
내/외부
네트워크
301
301
감시대상
(서버)
침입탐지시스템
데이터
수집부
302
312
감시대상
목록
저장부
데이터 필터링
및 축약부
303
313
감시대상별
보안정책
저장부
304
보안정책
위반탐지부
위반
허용
308
309
314
허용
305
위반
침입패턴
저장부
오용탐지부
결과조정 및
감사데이터
생성부
침입
대응부
315
306
프로파일
저장부
비정상행위
탐지부
위반
317
침입대응
규칙
저장부
316
307
위반
데이터
재분석
패턴
저장부
재분석부
311
보안관리부
경고 및
보고부
310

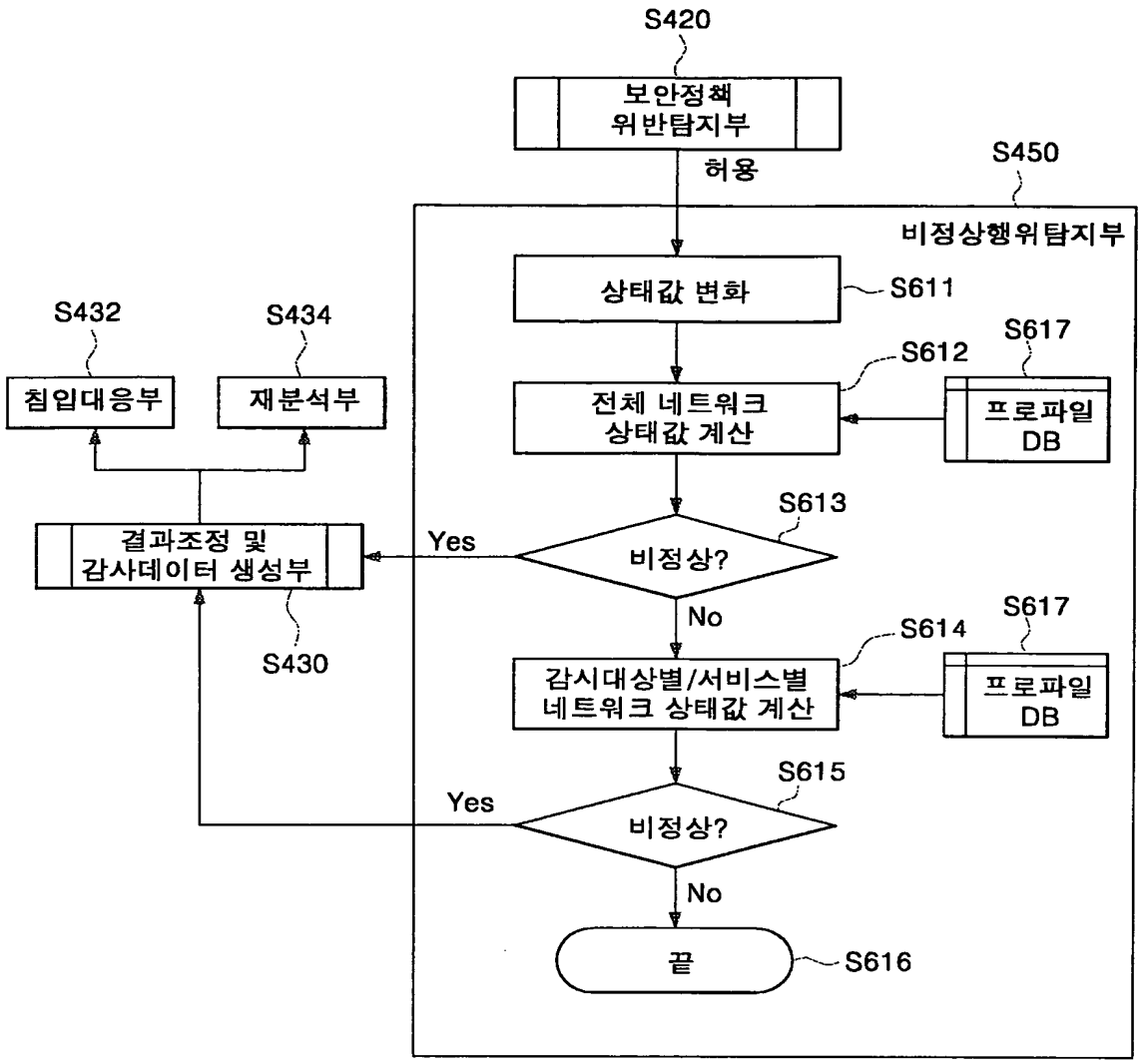
도면 4


데이터 수집부
S400
S410
데이터 필터링 및 축약부
S412
No
S411
패킷 Drop
감시대상?
감시대상 목록
S413
Yes
S420
보안정책 위반탐지부
S421
감시대상별 보안정책목록 검색
S422
허용정책
거부정책
감시대상?
S425
S423
S424
S426
허용목록
허용 서비스?
No
Yes
거부 서비스?
거부목록
Yes
No
결과조정 및 감사데이터 생성부
S430
침입대응부
재분석부
S432
S434
S440
오용탐지부
비정상행위탐지부
S450

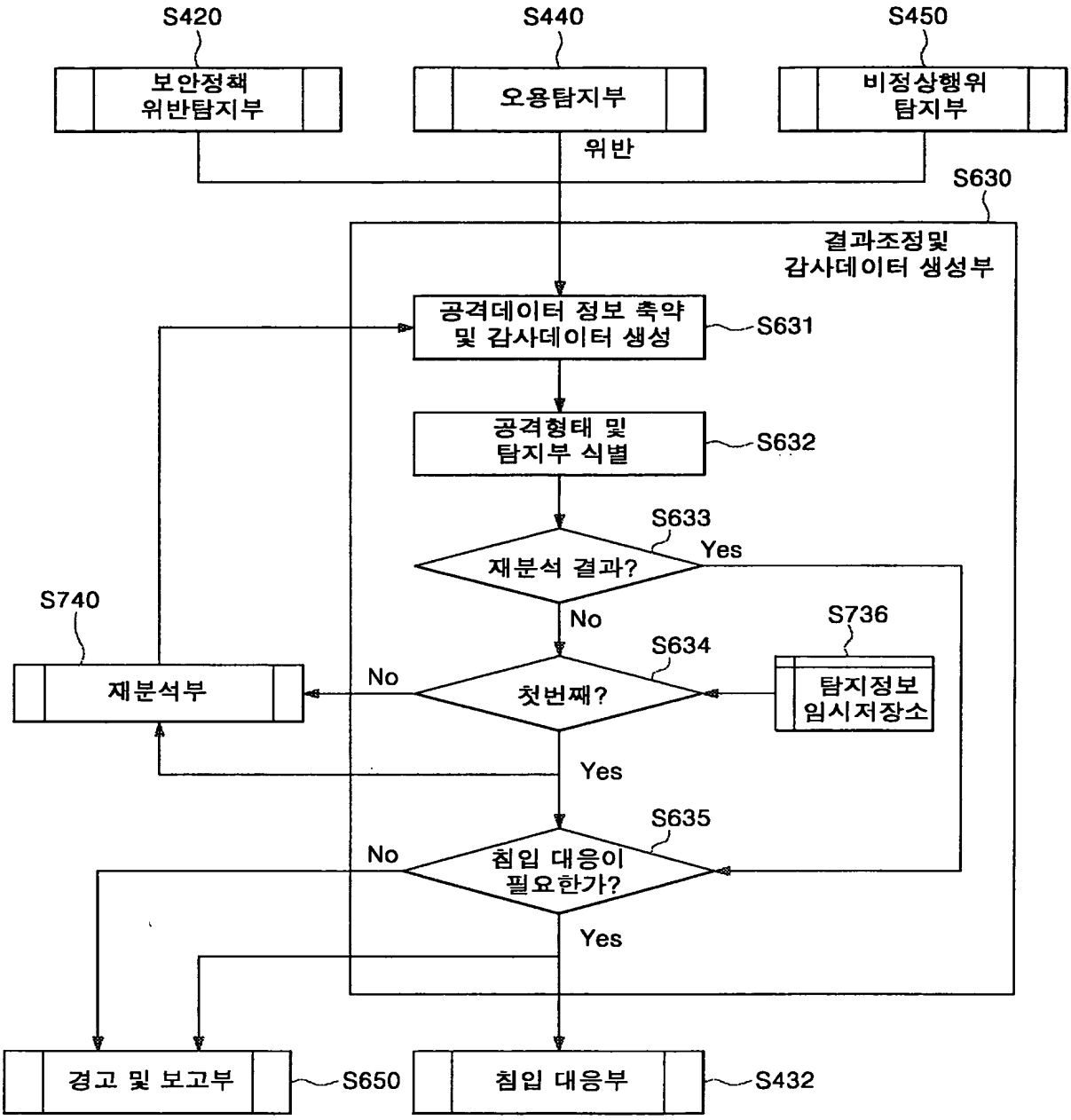
도면 5


S420
보안정책
위반탐지부
허용
S510
오용탐지부
S432
침입대응부
S434
재분석부
네트워크 프로토콜
관련 시그너쳐 추출
S511
S518
S512
네트워크
프로토콜 공격?
Yes
침입패턴
DB
No
결과조정 및
감사데이터 생성부
S430
응용서비스별 분배
S513
응용서비스별
시그너쳐 추출
S514
침입탐지 범위 설정
S515
S518
S516
응용서비스 공격?
Yes
침입패턴
DB
No
끝
S517

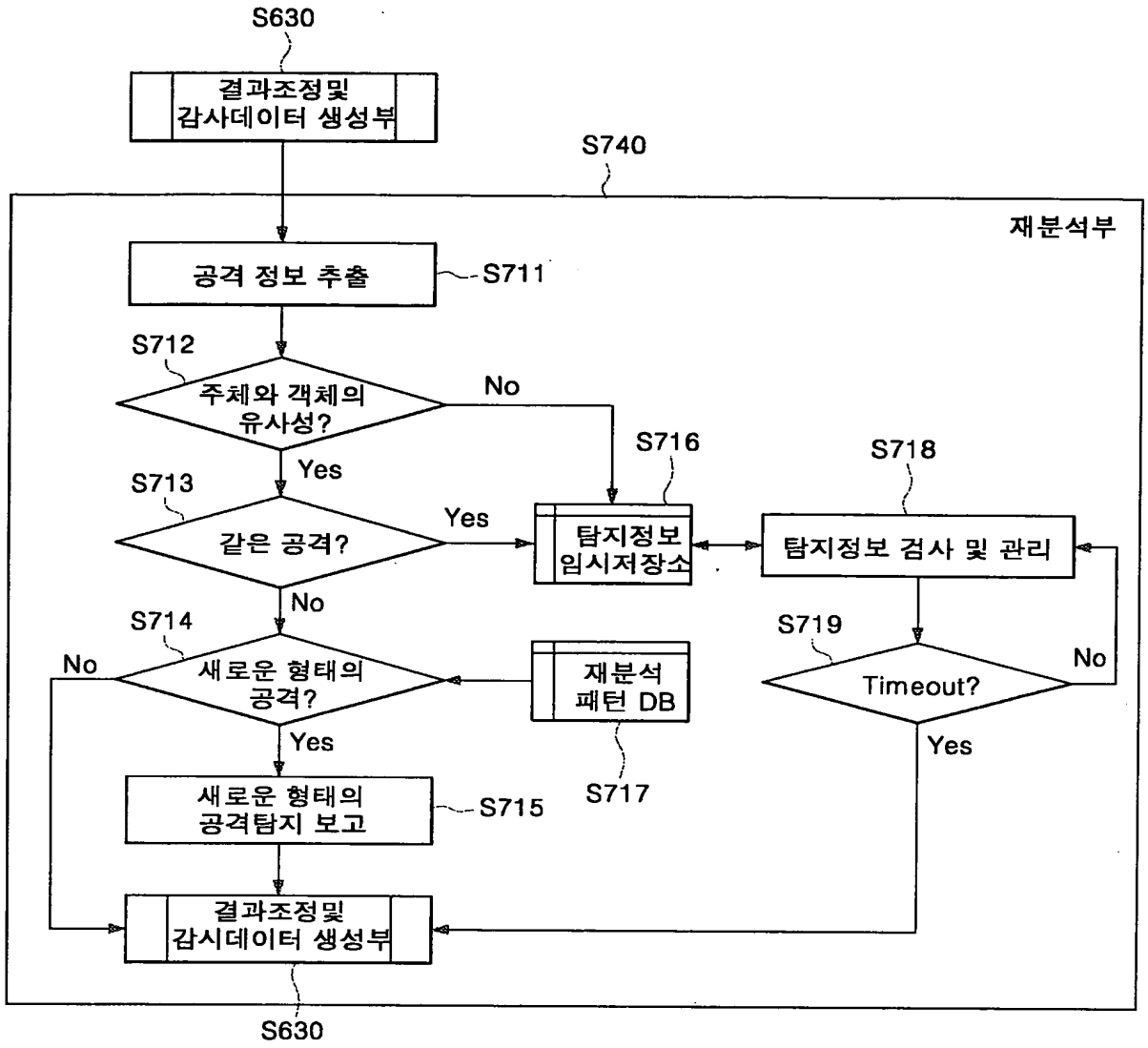
도면 6


S420
보안정책
위반탐지부
허용
S450
비정상행위탐지부
상태값 변화
S611
S617
S612
전체 네트워크
상태값 계산
프로파일
DB
S613
비정상?
Yes
No
S617
S614
감시대상별/서비스별
네트워크 상태값 계산
프로파일
DB
S615
비정상?
Yes
No
끝
S616
S432
S434
침입대응부
재분석부
결과조정 및
감사데이터 생성부
S430

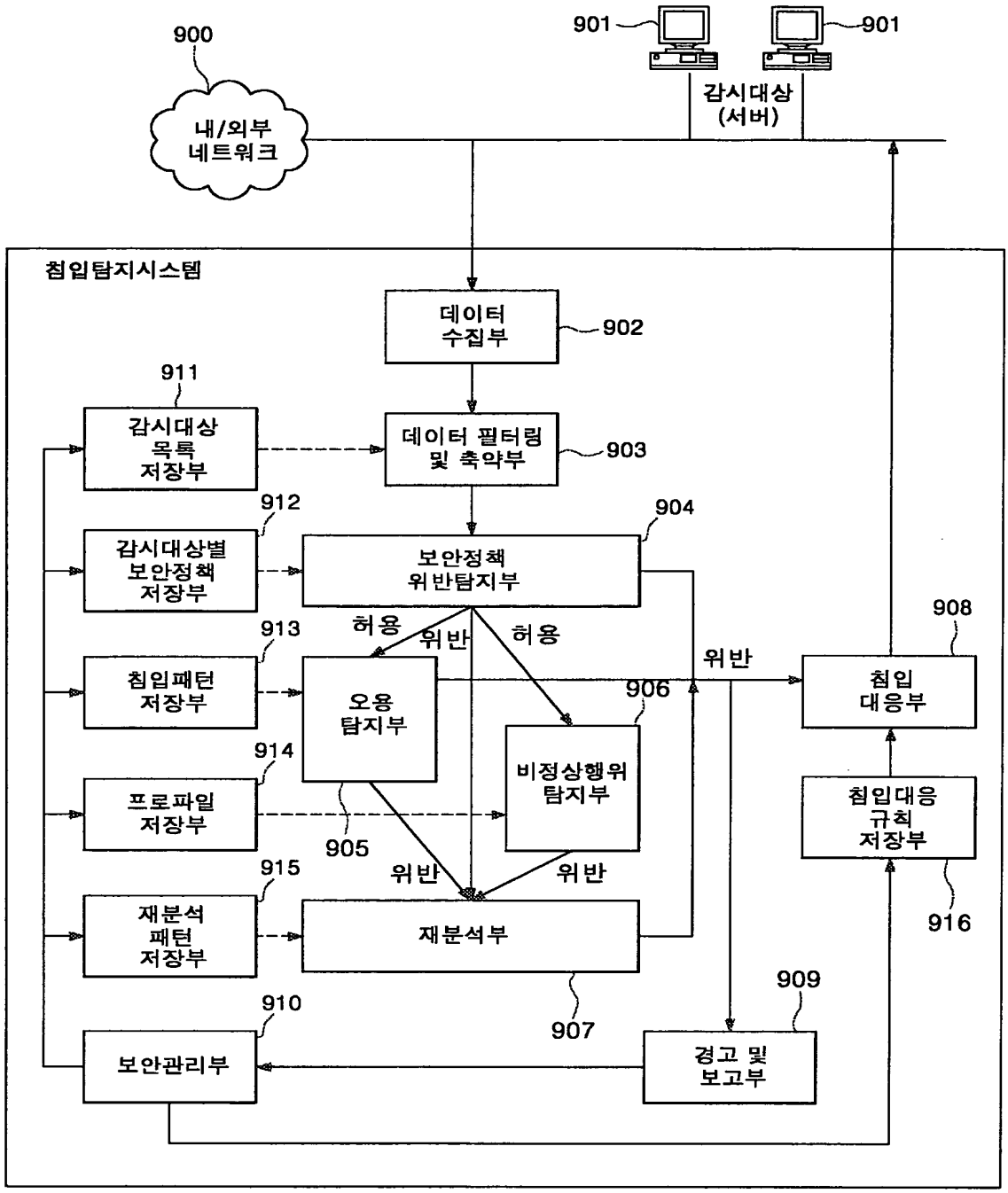
도면 7


S420
보안정책
위반탐지부
S440
오용탐지부
S450
비정상행위
탐지부
위반
S630
결과조정및
감사데이터 생성부
공격데이터 정보 축약
및 감사데이터 생성
S631
공격형태 및
탐지부 식별
S632
S633
재분석 결과?
Yes
No
S740
재분석부
No
S634
첫번째?
S736
탐지정보
임시저장소
Yes
S635
No
침입 대응이
필요한가?
Yes
경고 및 보고부
S650
침입 대응부
S432

도면 8


S630
결과조정및
감사데이터 생성부
S740
재분석부
공격 정보 추출
S711
S712
주체와 객체의
유사성?
No
Yes
S713
같은 공격?
Yes
S716
탐지정보
임시저장소
S718
탐지정보 검사 및 관리
No
S714
새로운 형태의
공격?
No
재분석
패턴 DB
S717
S719
Timeout?
No
Yes
Yes
새로운 형태의
공격탐지 보고
S715
결과조정및
감시데이터 생성부
S630

도면 9


900
내/외부
네트워크
901
901
감시대상
(서버)
침입탐지시스템
데이터
수집부
902
911
감시대상
목록
저장부
데이터 필터링
및 축약부
903
912
감시대상별
보안정책
저장부
904
보안정책
위반탐지부
908
허용
위반
허용
913
침입패턴
저장부
오용
탐지부
위반
906
침입
대응부
914
비정상행위
탐지부
프로파일
저장부
침입대응
규칙
저장부
905
위반
위반
915
916
재분석
패턴
저장부
재분석부
909
910
907
보안관리부
경고 및
보고부